Intrusion Detection Technique for Wormhole and Following Jellyfish and Byzantine Attacks in Wireless Mesh Network

K. Ganesh Reddy and P. Santhi Thilagam

Department of Computer Science and Engineering, NITK Surathkal, India
guncity11@gmail.com, santhisocrates@gmail.com

Abstract. Wireless Mesh Networks (WMNs) have emerging application because of its ad-hoc features, high internet bandwidth capability, and interoperable with various networks. However, all features of WMNs vulnerable due to their inadequate security services, and most of the existing techniques protect WMNs from single adversary node, but failed to protect colluding attacks. We proposed new Intrusion Detection (ID) technique, to protect the WMNs from wormhole attack (colluding attack) and following jellyfish and byzantine attacks. The proposed ID technique works based on different delays such as initial end-to-end packet delay, average end-to-end packet delay, and worst case end-to-end packet delay because wormhole attackers attract the network nodes by sending lower latency. Eventually, simulation results show that, our ID technique improves throughput of the network, when source and destination nodes detect and isolate (select new path which does not contain adversaries) the adversaries in wormhole attack and its following attacks.

1 Introduction

Wireless mesh networks (WMNs) have emerged as a key technology for providing fast and hassle free services to users and inspiring numerous applications. In recent years, wireless mesh networks have been becoming more popular because of its ubiquitous broadband wireless internet connectivity in a sizable geographic area and cost effective network deployment. WMNs have adorable features such as dynamic self-organization, self-configuration and self-healing. Fig. 1. depicts wireless mesh network architecture. Here all wireless radio nodes are connected in mesh to form infrastructure mesh and client mesh in which nodes are ordered hierarchy: gateway, router, and mesh client. WMNs can also interoperate with other wireless networks such as high speed metropolitan area mobile networks, backhaul connectivity for cellular radio access networks, intelligent transport system network defense system and citywide surveillance systems. A recent study shows that wireless mesh networks are more vulnerable especially in Network layer followed by MAC layer and Physical layer because of open medium, multihop wireless network, heterogeneous networks, dynamic topology and physical threat [3][4][5]. This paper, we addressed network layer attacks in

P.S. Thilagam et al. (Eds.): ADCONS 2011, LNCS 7135, pp. 631–637, 2012.

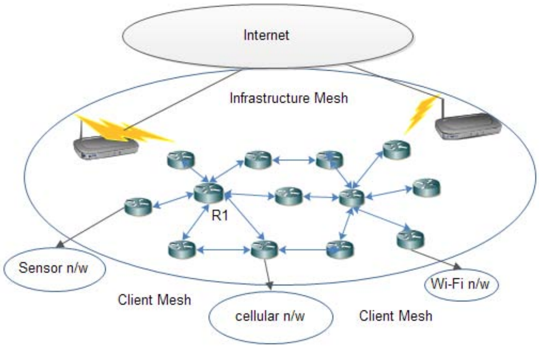

Fig. 1. Wireless Mesh Network Architecture

WMN. Network layer attacks are mainly classified into two types: control plane and data plane. Control plane adversaries affect the route discovery and maintenance phase of reactive, proactive, and hybrid etc. routing protocols. Here, adversary node creates attacks by itself such as blackhole, rushing attacks, or combine with other adversaries such as wormhole and colluding attacks. Moreover, all the adversaries are internal attackers, and to prevent these attacks existing prevention techniques are ineffective. Other alternative for this problem is Intrusion Detection (ID), many ID techniques have been proposed for single adversary attacks [2] [1]. But, very few existing ID techniques are available to protect colluding attacks (wormhole). However, these solutions are inadequate protect against the colluding attacks because these ID techniques suffers from false positive rate. And also, these techniques are developed for specific networks, and WMN cannot adopt these techniques directly. In this paper, we proposed new ID technique to detect wormhole attack, and its following attacks, and isolate the adversaries in the path from source to destination in WMN. Earlier, we proposed a challenge node technique solution for black hole attack but it is inadequate to protect wormhole attack [4]. In this current ID technique we overcome this problem, in which we consider three different delays between source and destination: initial end-to-end packet delay, average end-to-end packet delay, and worst case end to end packet delay. In the following, section 2 describes the wormhole attack and its following attacks; section 3 we explain proposed ID technique, Section 4 and 5 describes results, and conclusion.

2 Wormhole Attack and Its Following Attacks

Wormhole attack: Wormhole attack is formed by two colluding nodes in the network. To create wormhole attack any two mutual understanding malicious nodes form a tunnel with low latency and broadcast this information into the network. All overheard neighbor nodes send data packets through the tunnel, and then malicious nodes extract the important data from the data packets or